SPECIFICATION

1. **Mobile data extraction, decoding and reporting tool with 3 Years License**
(The Mobile forensic solution as referred in this document includes both central monitoring unit and / or User as applicable)

S.No	Mobile data extraction, decoding and reporting tool
1	The mobile forensic solution should offer choice of software license or USB hardware dongle (CodeMeter) license. Software license for enterprise solution.
2	The mobile forensic solution should be a flexible Software Solution allowing its installation on any of the Organization's compatible PC running a supported Windows Operating systems, thus avoiding any need for purchase of any additional proprietary hardware equipment to execute core extraction and decoding features.
3	The mobile forensic solution should be independent of any vendor-specific extraction hardware component(s) that could act as a single point of failure and potentially block the buyer's capability of extracting mobile device data in case of malfunction of such component.
4	The mobile forensic solution (client) should allow immediate display of the extraction process results (such as chat conversations, calls, browser history, geographic data and others) without any additional data processing steps with long waiting times each time the extraction is opened for analysis, avoiding delays in data analysis tasks
5	The mobile forensic solution (client) should be able to extract at least 3 mobile devices simultaneously.
6	Forensic solution(client) should automatically generate a detailed audit log file of the forensic process for each extraction for peer review.
7	The mobile forensic solution should use Windows Certified and signed USB drivers to avoid interference with any other software running on the computer and for IT Security, this information must be available on Microsoft's windows compatible product list. Relevant reasons: https://docs.microsoft.com/en-gb/windows-hardware/drivers/develop/signing-a-driver
8	The mobile forensic solution should have at least 50,000+ mobile device profiles. It should support more than 470 Applications and 4650+ different versions of these applications.
9	The mobile forensic solution should support at least the following applications: WhatsApp, GB WhatsApp Pro, NS WhatsApp, OG WhatsApp Pro, WhatsApp Business, Telegram, Graph Messenger, MoboGram Viber, Facebook, Messenger, Instagram, Kik, KakaoTalk, Wire, Calculator#, Microsoft Teams, +Message, MeWe, Slack, Line, Skype, WeChat, Google Duo, QQ Browser, Session, Threema, Signal etc.
10	The mobile forensic solution should support Application Downgrade Method on various Android OS non-system applications. Applications supported for downgrade must include apps : Whatsapp, Skype, TrueCaller, Telegram, ElGramiMessenger, WeChat, Instagram, KakaoTalk, Line, Facebook Messenger, Facebook, Houseparty, QQ, Signal, imo etc.

19/04/25 19/04/2025 19/04/25

10	The mobile forensic solution should support Application Downgrade Method on various Android OS non-system applications. Applications supported for downgrade must include apps : Whatsapp, Skype, TrueCaller, Telegram, ElGramiMessenger, WeChat, Instagram, KakaoTalk, Line, Facebook Messenger, Facebook, Houseparty, QQ, Signal, imo etc.
11	The mobile forensic solution should perform various logical extraction methods like Agent, Backup, Filesystem and app downgrade all in one go and user need not to perform each method i.e. Agent, Backup, Filesystem and app downgrade Seprately.
12	The mobile forensic solution should have capability to modify existing profile's or create a new profile and configure extraction and decoding option based on user requirements.
13	The mobile forensic solution should have feature to specify the time span allowing to limit all the artifacts in extraction to a certain time span.
14	The mobile forensic solution should have feature to select all apps or a limited set of apps to include in the extraction.
15	The mobile forensic solution should feature to specify categories like Messages, Calls, Accounts etc. to reduce the extraction time and size by excluding non-important artifacts categories.
16	The mobile forensic solution should support Rapid hash match functionality that enables to acquire information about the device data before the extraction has even finished. Hash matching functionality should support MD5, SHA1 and SHA 256 hash algorithms.
17	The mobile forensic solution should provide options for support of mobile devices via Generic Profiles to allow for support of new and untested devices. Required generic profiles : a) Android generic, Apple iOS generic, RIM Blackberry generic, Windows generic. b) Android MediaTek generic, Spreadtrum Android generic, Qualcomm EDL generic, Huawei Kirin generic. c) Mediatek generic, Spreadtrum generic, Coolsand generic, Infineon Generic, Garmin Gps portable generic. d) LG Qualcomm generic, Sony android generic, Fujitsu Android Generic, Kyocera Android Generic.
18	The mobile forensic solution should support data extraction from Android devices via Wi-Fi interface, thus covering the situations when cable connection is not possible due to malfunction of device's data connector.
19	The mobile forensic solution should support indexing of certain readable file formats (such as pdf, docx, xlsx, sqlite databases, xml, txt, html, log) during the decoding process, so that Operator could have possibility to perform text-based searches and get quick results if matches exist in files of such formats
20	The mobile forensic solution should examine file headers for the data acquired from the device in order to determine the correct format (type) of the extracted files, and not rely on file extensions. This must apply to any type of extraction performed for the supported devices.
21	The mobile forensic solution should have speech-to-text capability for audio file and video file which is supported by Ffmpeg or equivalent and utilising Nvidia GPUs to accelerate the speed.

19/04/2025 19/04/2025 19/04/25

22	The mobile forensic solution should support extraction of text-searchable data in any language , covering all major languages (data such as chat messages, profile descriptions, etc.) from applications WhatsApp, Signal, Telegram, WhatsApp Business running on Android 6 or newer, by means of automated screenshot taking. All the instances of these apps should be supported.
23	The mobile forensic solution should support a generic extraction method of text-searchable data in any language from other untested applications which permit taking screenshots and vertical scrolling, and are running on Android 6 or newer, by means of automated screenshot taking
24	The mobile forensic solution should be able to extract vital application data on device running but not limited to below OS: • iOS • Android • Blackberry OS • Windows Phone/Mobile/CE/RT • Asha Platform • KaiOS • Tizen OS • Symbian OS • Bada OS • Palm OS
25	The mobile forensic solution should enable physical extraction and decoding of data from a range of portable GPS devices. The Decoded data should include: Active Log, Favourite Waypoints, Route Waypoints. Supported GPS devices must include (but not limited) the following models: Garmin eTrex, Garmin eTrex 10, Garmin eTrex Legend, Garmin eTrex Vista C, Garmin eTrex Vista Cx, Garmin eTrex Vista H, Magellan eXplorist GC , Magellan eXplorist 710, Magellan Maestro 3235, Magellan maestro 4040, Magellan Roadmate 1200, Sony GPS CS1, Sony GPS-CS3, Sony NV-U70T etc.
26	The mobile forensic solution should enable physical extraction and decoding from various feature phones. Supported features phones must include (but not limited) the following models : Nokia 105 TA-1299, Nokia 105 TA-1304, Nokia 105 TA-1294, Nokia 106 TA-1190, Nokia 110 TA-1192, Colors Cl101, Itel IT 2160, Itel It 2123, Itel it 2180, Blackzone b313 Gold, Blackzone genius X, Spy Gadget Dual sim GSM Box, Lava Captain N1, Lava Capatin N1 Lite, Snexian Rock, Kechaoda K112 Tri SIM, Intex Turbo 108+, White cherry BL3100, etc.
27	The mobile forensic solution should enable physical extraction with lock bypass on various Android phones.Supported devices must include (but not limited) the following models: Lenovo A6600 A6600d40, Oppo A37m Dual SIM, Oppo F1s Global Dual SIM, Sony Xperia C4 dual LTE E5333, Sony Xperia C4 dual TD-LTE E5363, Sony Xperia C4 LTE E5306, Sony Xperia C4 TD-LTE E5353, Tecno F1 Dual SIM (VP510), BBK vivo V5 Lite (1609), LAaboo T6, Celkon Diamond 4G etc.

19/04/2025 19/4/25 19/04/2025 19/04/25

28	The mobile forensic solution should enable physical extraction and decoding from various feature phones based on Unisoc UMS9117 - T117 and UMS9107 - T107 chipset. Supported devices must include (but not limited to) Nokia 105 4G 2023 DS (TA-1551), Nokia 105 4G DS (TA-1378), Nokia 110 4G (TA-1386), Sky Devices F4G etc.
29	The mobile forensic solution should allow users to perform a Physical / full file system with Lock bypassing/Bruteforcing on smartphones with the Huawei HiSilicon KIRIN chipset. Supported range of Chipsets must include Kirin 990, 980, 970, 960, 950, 930, 920, 910, 810, 710, 650 & 620 Chipsets. For Huawei and Huawei Honor device must be running android 7, 8, 9, 10 and 11.
30	The mobile forensic solution should support data extraction for ios devices. It must have option to bruteforce encrypted iTunes backup.
31	The mobile forensic solution should support "full filesystem" extraction for iPhone 8, iPhone 8 Plus and iPhone X running latest till iOS 14. The mobile forensic solution should allow taking screenshots from Apple devices without the need of manually installing any additional application on the examined device
32	The mobile forensic solution should have a image content recognition capability and utilising NVidia GPUs toaccelerate image classification times.
33	The mobile forensic solution should have support to extract full file system from unlocked Android devices. It should also have generic profile to extract full file system from untested and unlocked Android device
34	The mobile forensic solution should have options for export of data into the standard file formats of XLS, PDF, WORD, GPX, KMZ, VIC, FILE, EXTENDED XML, HTML, OpenDocument Text, OpenDocument SpreadSheet, Nuix.
35	The mobile forensic solution should have a fully reference documented manual for the product that: a) Manually lists all devices and apps supported via the extraction software to aid investigators; b) List what data types can be extracted on specific device profile; c) List what data types cannot be extracted on specific device profile; d) Available via mobile phone app to manually lists all devices and apps supported to aid investigators.
36	The mobile forensic solution should have a fully documented reference manual that lists out the device or application based on: a) Device Type; b) Manufacturer; c) Form Factor; d) Device Operating System; e) Application Category; f) Application Operating System.
37	The mobile forensic solution should support advanced and rapid data analysis and filtering features, applicable to multiple extraction files groupped together by the Operator in any combination. Maximum number of extraction files accepted for simultaneous analysis must not be limited by The mobile forensic solution, but only by available computer resources

19/09/25 19/9/25 19/09/2025 19/09/25

38	The mobile forensic solution should have Optical character recognition (OCR) feature to automatically decode the text in pictures and generate searchable text.
39	The mobile forensic solution should have Pre-scan feature to scan and show the detailed information of the device prior to extraction. Pre scan info must show Device Make/ Model, Serial No, OS version Security patch Level Installed apps etc. In pre- scan information apps should be divided into various categories like, finance, communication etc.
40	The mobile forensic solution should be able to provide a Conversation view Visualization , Connection (Link Analysis) View Visualization, Time Line View Visualization & Map View Visualization.
41	The mobile forensic solution should be able to import Call Data Records.
42	The mobile forensic solution should have Persons' AI Capability, Unique intelligent core decoder able to present and link multiple identifiers to a single person identity. The mobile forensic solution should have participant filter for tracing a conversation that includes many persons using different message apps.
43	The mobile forensic solution should have solution to import warrant returns from Apple, Coinbase, Facebook, Google, Instagram , Snapchat, Etc.
44	The mobile forensic solution should support additional decoding capabilities (manual and automated) of extracted data. The Operator must have at least the following 3 ways available: Direct manual decoding via examiner software interface of raw source data Automated decoding via Python scripts, with supported Python version being at least 3.7 or higher. Guided decoding with special wizard-based interface for decoding sqlite database tables data
45	The mobile forensic solution should have language detection feature to analyze text and identify the languages.
46	The mobile forensic solution should have feature to integrate offline Maps.
47	The mobile forensic solution should let users connect all their mobile forensic extraction tools into a single network.
48	The mobile forensic solution should let user control all of their mobile forensic system from one central location, pushing out watch lists and new software updates, monitoring users and processes, and creating management information reports and hash lists.
49	The mobile forensic solution should let user remotely review the logs for all devices in your system to see who performed what function and when.
50	The mobile forensic solution should provide tailor-made reports of vital management information that let you make more informed decisions and allocate resources better. An easy way to find and follow up on KPI's.
51	The mobile forensic solution should let you update software, manage licenses and select automatic update routines for entire systems from one place. It should also allow remote diagnostics and the possibility of assisting users experiencing difficulties.

19/04/2025 19/4/25 19/04/2025 19/04/25

52	The mobile forensic solution should allow to see and manage all active users in system remotely, for example by creating, adding or deleting users, defining their individual permissions and managing their workflows, grouping them and setting standardized group permissions and so on.
53	The mobile forensic solution should be capable of managing the connected Frontline Extraction Platforms, Investigator Analysis Software Solution and the Expert Extraction Platforms.
54	The mobile forensic solution should allow centralized review of logs for all Extraction/Analysis Software Solutions connected.
55	The mobile forensic solution should be able to perform various tasks like- a) Define the validity period of the Token for the system / client b) Remove a system / client c) Update software for each clients d) Renew the license for all clients e) Get the connection and extraction log f) Generate system activity report
56	The mobile forensic solution should have scalable License solution system based on Server / Clients
57	The mobile forensic solution should be licensed locally via a software license key and should not be hosted on any OEM cloud server.
58	The mobile forensic solution should have batch exporting capability using a standalone tool for this function.
59	The mobile forensic solution should export multiple files to alternative data formats like PDF, Word, excel, Extended XML, VICS, KMZ, Nuix etc.
60	The mobile forensic solution should allow running export process as a background service.
61	The mobile forensic solution should have 50 Total enterprise users and each user should be provided with full Connection Kit & should have 20 Concurrent Users.
62	The software must have 3 Years License
63	Extracted Data should not go to any other system except local user's system.
64	Minor customization of the monitoring report should be on the monitoring server as per requirements.

19/04/2025

19/04/2025

19/4/25

19/04/25

2. Comprehensive Digital Investigation platform for Forensic Data extraction and analysis of live system, Hard drives, Mobile phones & Cloud with 3 Years License

SL	COMPREHENSIVE DIGITAL INVESTIGATION PLATFORM FOR FORENSIC DATA EXTRACTION AND ANALYSIS OF LIVE SYSTEM, HARD DRIVES, MOBILE PHONES & CLOUD
1	A robust platform designed for comprehensive data extraction and analysis, capable of handling a wide range of sources such as real-time acquisition, memory analysis, computers, cloud resources, mobile devices, and vehicle data.
2	The solution should support at least five concurrent users and offer scalability to accommodate any future expansion.
3	The licensing model should be cloud-based, accessible via activation code at any time, and should support offline usage for a defined period after activation.
4	It should allow installation on multiple machines, with simultaneous usage limited to the number of licensed concurrent users.
5	Offers customized workflows optimized for Windows, macOS, and Linux environments to ensure seamless compatibility and high performance across platforms.
6	Supports data acquisition from Android devices, along with logical extraction from iOS devices, Windows phones, MTP devices, SIM cards, and Kindle devices.
7	Extends compatibility to major Linux distributions, including Ubuntu, Debian, Red Hat, Kali, and others, covering a broad spectrum of operating systems.
8	Allows export of vehicle forensic data in the .ivo file format, enabling users to merge data with other sources within a single case for streamlined analysis of waypoints, routes, velocity logs, contacts, call logs, connected devices, and more.
9	Supports physical memory acquisition (RAM dump), enabling the retrieval of volatile data and artifacts typically found only in memory.
10	Includes functionality to capture memory from individual running processes, offering a targeted approach for specific investigations, improving efficiency and recovery of larger data types.
11	Provides a tool (commandline or gui) for quick and discreet identification of encrypted volumes on suspect systems during incident response.
12	Capable of analyzing memory dumps without size limitations.
13	Supports full disk decryption, with the ability to detect and decrypt TrueCrypt, BitLocker, McAfee, VeraCrypt, and FileVault2 using known passwords or brute-force methods.
14	Enables automatic queuing and processing of multiple devices (at least 10) sequentially, eliminating the need for manual intervention between devices.
15	Includes a built-in SQLite viewer for direct access and review of SQLite database files.
16	Supports Optical Character Recognition (OCR) for extracting text from PDF files—including scanned documents and embedded images—as well as from picture artifacts for effective keyword searching.
17	Should support search for keywords on both recovered artifact and sector level content both prior to processing the case as well as after processing the complete case with an option to select all added evidence sources or any particular evidence source.
18	Ability to identify luring and sexual conversations. 15+ AI Categories to automatically identify and bifurcate images related to drugs, weapons, nudity, weapons, militants, vehicles, screen captures, documents, ID Cards, Human Faces, License Plates, Building, Child Abuse, Tattoos, Invoices, etc
19	identify and categorize handwritten documents automatically with AI.
20	support CSAM investigations with AI technology, and help you uncover key evidence even more quickly Including new AI technology from Thorn to identify illicit content leveraging their CSAM Image Classifier to improve the detection of CSAM across picture and video artifacts.

19/04/25 19/04/25 19/03/2025 19/04/25

21	Inbuilt Support for finding similar pictures by building picture comparison for identifying any similar pictures from the extracted images or external images using CBIR (Content Based Image Retrieval) feature
22	Should have advance option to analyse media file using dedicated Media explorer to view, sort, and filter media evidence using criteria that are specific to pictures and videos. The Media explorer should stack copies of the same picture or video that were found in different source locations.
23	ability to hover over image/video, which should provide a larger, higher resolution preview of the image or video. Users can also zoom and pan around an image within the preview. For videos, investigator should be able to use the mouse to quickly scroll through the contents of the video.
24	Should have utility which can be installed on any number of Windows Tablet or Laptop to empower frontline officers to collect and report on fleeting digital evidence. The tool should be capable to Maintain privacy and build trust with the public while capturing crucial but fleeting digital evidence from consenting victims and witnesses.
25	Quickly get Photo, video evidence with an external or internal camera or by connecting to the victim or witness's mobile phone, or memory card.
26	Support case dashboard that displays high level details about the case, evidence sources and summaries of processed results of multiple digital evidence in one screen.
27	**Visualize connections between files, users, and devices.** Discover the full history of a file or artifact to build case and prove intent. visualizes evidence from disk and memory to show where files came from, who they are connected to, and where they're stored.
28	Should support parse and carve and parse selected artifact option to save time on a case if carving is not necessary for investigation.
29	Should have Timeline explorer to consolidate all the timestamps from files and artifacts in a single view, with colours and tags to differentiate timestamp categorizes.
30	Ability to automatically find potential chat databases along with other valuable evidence from non-chat apps that aren't yet supported in an artifact. users can then easily create an XML or Python artifact to be searched for in future cases.
31	Capability for parsing unsupported database using custom artifacts or Python Scripts for popular local applications like Tally, Airbnb, CCleaner, FakeGPS, Linkedin, onion browser bookmarks etc.
32	Should have a GUI/Wizard-driven utility, so no coding experience required to build custom artifacts CSV/Delimited files (tab-separated, space-separated, or custom delimiters) and SQLite databases to bring data into the offered tool from other sources without needing to know XML/Python or API.
33	Should have a platform that allows forensics professionals access to repository of Custom artifacts and option to upload custom scripts that they have built, and help their peers with their cases, or download artifacts others have built to help with their own cases.
34	Add hash sets to either filter out non-relevant files to enhance search performance and reduce false positives or add hash sets that will specifically call out and identify known bad pictures and videos.
35	Should have an Animated Map feature to show the user's movement based on the geolocation information from device data, combining location and timestamp data to show the path they took during a given time frame.
36	Support to export & merge portable case and share with other stakeholders without the need for the software license or the need to install the software, the user can select different types of items to be included according to tags, comments and categories.
37	Should be capable to acquire evidence from the cloud, by sign in to an account with the target's user name and password, or—for some platforms—an authentication token that the tool discovers during a search or creates itself.
38	Should support cloud based Data acquisition from popular Cloud services, including iCloud,MS Office365, POP/IMAP emails, Facebook, Twitter, Google, Slack, Instagram, Box, Dropbox, Microsoft Teams, Uber, Lyft, Mega etc.

19/04/25 19/04/25 19/04/2025 19/04/25

39	Should have ability to acquire public data from Twitter and Instagram without knowing the targeted user's credential.
40	Should Support ingesting the downloaded user data package from Facebook, Google and Slack.
41	Should Support analysis of warrant return from Google, Facebook, Instagram, Snapshot and iCloud.
42	Should have option to save cloud acquisitions to AFF4-L containers.
43	The software must have 3 Years License

3. Forensic Duplicator with 3 years Warranty

SL	Forensic Duplicator with 3 years Warranty
1	Forensic Duplicator should have: • Three write-blocked source ports: SATA/SAS, PCIe, and USB 3.2 (Type-C). • Five destination ports: SATA (x2), PCIe, and USB 3.2 (Type-C, x2) • One USB (Type-C) accessory port
2	Should have color, touch-screen LCD
3	Should support forensic imaging of SATA/SAS, USB, IDE, FireWire, m.2/NVMe.
4	Should have hot-swap PCIe source and destination devices
5	Should be single device imaging, output to up to five (5) destination devices
6	Should have audible and visual job status feedback feature.
7	Should have administrative options to set features by user
8	Should support Disk-to-disk (clone), disk-to-file (imaging), and logical device imaging.
9	The duplicator should provide the following Output image files types: RAW/DD, E01, EX01, DMG
10	It should have a support for various file systems (Input: output) FAT32, EXFAT, NTFS, HFS+, EXT4
11	Should have MD5, SHA-1, and SHA-256 hashing support.
12	Should be able for detailed job logs for view, print, and export
13	Should have encryption detection feature with key unlock
14	Should support secure output using AES-256 encryption
15	Should support multi-file system detection and browsing
16	Should support AMA/HPA/DCO detection and hidden partition removal or unlock
17	Below mentioned accessories should be present with the Forensic Duplicator • TC4-8-R4 (x3) unified SATA/SAS signal and power with molex connection • TC-PCIe-8 PCIe adapter cable, 8" • TCA-USB3-AC (x2) USB Type-A to USB Type-C adapter cable • Cleaning cloth • Quick reference guide
18	Forensic Media Card Reader – Must include Forensic Media Card Reader with Read Only and Read Write Switching Capabilities.
19	Warranty including Firmware/ Software updates for 3 Years. Any Software/ Firmware updates to be provided during the Warranty Period.
20	Product Offered should be of International Repute & Brand and should not be customized/ assembled Product from various sources.

19/04/2025 19/4/25 19/04/2025 19/04/25

SPECIFICATION

1. Forensic Workstation Desktop with 3 Years Warranty

SL	Forensic Workstation Desktop with 3 Years Warranty	
1	Product	Forensic Workstation Desktop
2	Processor	Intel core ultra 5/7/9 or it's equivalent AMD processor
3	Chipset	Intel Workstation / AMD Workstation
4	Memory Slot	4 DIMM
5	Memory	128GB (4x32GB) DDR5 4400 UDIMM ECC Memory or better
6	Graphics	NVIDIA® RTX™ 2000 Ada, 16 GB GDDR6
7	Storage	1 x 1TB PCIe-4x4 2280 M.2 Solid State Drive 1 x 2TB M.2 Solid State Drive
8	Input Device	USB Keyboard Wired Optical Mouse
9	Communication	Intel AX211 Wi-Fi 7 +Bluetooth 5.4 WW WLAN with Internal Antennae
10	Audio	Realtek ALC3205-VA2-CG, 2.0W internal mono speaker or equivalent
11	Ports & Connectors	**Front:** 1 USB 3.2 Gen 1 (5Gbps) port 1 USB 3.2 Gen 1 (5Gbps) port with PowerShare 1 USB 3.2 Gen 2 (10Gbps) Type-C port 1 USB 3.2 Gen 2x2 (20Gbps) Type-C port with PowerShare 1 Global headset jack 1 SD 7.0 Express-card slot (Optional) **Rear:** 2 USB 2.0 (480Mbps) ports with SmartPower 2 USB 3.2 Gen 2 (10Gbps) ports 1 USB 3.2 Gen 2x2 (20Gbps) Type-C port 1 RJ45 (1GbE) Ethernet port 2 DisplayPort 1.4a HBR3 ports 1 Optional port (TBT4 (40Gbps) + USB-C (10Gbps) data , DP alt-mode Type-C (10Gbps), HDMI 2.1, DP 2.1, 5Gbe LAN, 2x USB-A 3.2 (10Gbps), VGA, 5GbE Optical)
12	Expansion Slot	4 SATA 3.5-inch HDD/ODD 2 M.2 2230/2280 PCIe Gen4 slots 1 M.2 2230/2280 PCIe Gen5 slot 1 PEG full-height Gen5 PCIe x16 slot 1 full-height, half-length Gen3 x4 PCIe closed-end slot 1 full-height, full-length Gen4 x4 PCIe open-end slot 1 full-height, full-length Gen3 x4 PCIe open-end slot
14	Certification	ENERGY STAR certified or it's equivalent
15	Operating System	Microsoft Windows 11 Professional High End. Licensed Factory pre-installed certificate for Windows 11 Professional should be furnished on OEM Letter with the bid and Linux (Red Hat/SUSE) certified.
16	Power Supply	500W internal power supply unit (80PLUS Platinum Certified)
17	Monitor	23" Monitor FHD, 1920 X 1080, IPS, 350 nits, DisplayPort 1.2,1 HDMI 1.4, 4 USB-A 5Gbps(1 Charging), EPEAT, Energy star, TCO Certified
18	Security	Antivirus, Multilayer Ransom ware & Antimalware Protection, protection, Advanced Threat Defense, Cloud Management, Secure Browsing

25/04/25

25/04/2025 Director. CFDFEL

Gyanasindhu Sahoo S/I of Police 25/04/25 CFDFEL

Sanat Kumar Nayak Inspector of Police 25/04/2025

		(Online Threat Prevention), File Shredder, Powerful Anti-Phishing, USB Immunizer, Password Wallet, Safe Online Banking, Anti-Tracker, 1- Click Optimizer, Automatic Upgrades
19	Certifications	Desktop Workstation OEM should have valid ISO9001, ISO50000, ISO20001, ISO27001, ISO14000 BEE/Energy Star certificate, FCC, EPEAT India and TCO for Monitor, MIL Standard, Microsoft Windows 11 and Linux (Red Hat/SUSE) certified. & Specific Data Sheet .
20	Products	OEM should have same make of Keyboard, Mouse, Monitor, and CPU. OEM LOGO /trade mark should be embossed on them (No sticker will be accepted) for Workstation. OEM should be from IDC TOP 3 Desktop Workstation Brand
21	Warranty	3 years onsite warranty

2. Uninterruptable Power Supply Device

SL	Power Protection Device	
1	Capacity (in kVA / kW)	3 kVA/2.4kW 1-Phase Input / 1-Phase Output with IGBT Rectifier
2	Input Voltage Range	110-300VAC
3	Input Frequency Range	40 - 70Hz
4	Nominal Output voltage	200/208/220/230/240 VAC
5	O/P Voltage	200/208/220/230/240Vac
6	Min Inbuilt Charger	6Amp or above
7	Efficiency (Min)	90% at full load
8	Output Socket	Output Socket. Minimum 2nos - Indian Socket & 1 Terminal Block inbuilt to the UPS back
9	Backup Required	Min.3024 VAH for 30min.
10	Battery Bank Voltage	72 VDC
11	USB Port should be available	Yes
12	RS232 & SNMP Port	Yes
13	Product IP	IP 20
14	Inbuilt Automatic Bypass	Yes
15	Intelligent Battery Management	Yes
16	Battery Deep Discharge Protection	Yes
17	ECO Mode	Yes
18	Manufacturer Certification	QMS: As per ISO 9001: 2008 EMS: As per ISO 14001: 2004 ISO 45001:2018 TL9000 Factory calibration lab of manufacturer shall be NABL accredited in India
19	ROHS	Yes
20	3 Years Warranty for UPS & 2 Years on Battery.	

25/4/25

25/04/25
Dy. CFDEEL

Gyanendra Sahu
Dy of Police
CFDEEL
25/04/25

Sanat Kumar Nayak
Inspector of Police
25/4/2025